A Modular Analysis of the Fujisaki-Okamoto Transformation

Research Seminar Cryptography, Fall 2018

Reelika Tõnisson

Supervised by Dominique Unruh

Abstract. This report gives an overview on the work done by Hofheinz, Hövelmanns and Kiltz [1]. They provide a toolkit of transformations for turning weakly secure into strongly secure public-key encryption schemes. They also analyze the transformations in the quantum random oracle model, which yields security guarantees in a post-quantum setting.

1 Introduction

The notion of INDistinguishability against Chosen-Ciphertext Attacks (IND-CCA) is known as the standard security notion for asymmetric encryption schemes. Intuitively, IND-CCA security requires that no efficient adversary can recognize which of two messages is encrypted in a given ciphertext, even if the two messages are chosen by the adversary himself. In a similar but weaker notion of INDistinguishability against Chosen-Plaintext Attacks (IND-CPA), adversary is not given access to a decryption oracle throughout the attack.

IND-CCA is the desired notion of security in many applications, but it is usually much more difficult to prove than IND-CPA security. Thus, several transformations have been suggested that turn a weaker public-key encryption (PKE) scheme into an IND-CCA one generically. For instance, in a seminar paper, Fujisaki and Okamoto [3, 4] proposed a generic Fujisaki-Okamoto transformation (FO transformation) combining any One-Way (OW-CPA) secure asymmetric encryption scheme with any one-time secure symmetric encryption scheme into a hybrid encryption scheme. OW-CPA security requires that no efficient adversary can find the encrypted message based on the ciphertext and public key. That hybrid scheme is (IND-CCA) secure in the random oracle model.

Subsequently, Okamoto and Pointcheval [5] and Coron et al. [6] proposed two more generic transformations (REACT and GEM) that are considerably simpler. These however require the underlying asymmetric scheme to be One-Way against Plaintext Checking Attacks (OW-PCA). OW-PCA security is a non-standard security notion that provides the adversary with a plaintext checking oracle $Pco(c, m)$. Pco returns 1 iff decryption of ciphertext c yields the original message m.

A Key-Encapsulation Mechanism (KEM) is a probabilistic algorithm that produces a random symmetric key and an asymmetric encryption of that key. Any IND-CCA secure KEM can be combined with any (one-time) chosen-ciphertext secure symmetric encryption scheme to obtain a IND-CCA secure PKE scheme. Due to the efficiency and versatility, in practice one often works with hybrid encryption schemes derived from a KEM. For that reason the primary goal of the paper will be constructing IND-CCA secure KEMs.

In many cases, cryptosystems that use hash functions are very difficult or even impossible to prove based only on simple assumptions about the hash function (like collision-resistance). Instead, we would like to use the fact that a hash function behaves like a totally random function. That is called analyzing protocols in the Random Oracle Model (ROM). So, instead of using a hash function $H : M \to N$, we model the hash function as a uniformly randomly chosen function out of the space of all functions from M to N. This randomly chosen function is called a random oracle.

We also consider security games in the Quantum Random Oracle Model (QROM). The difference from classical ROM is that we consider quantum adversaries that are given quantum access to the random oracles involved, and classical access to all other oracles (e.g., plaintext checking or decapsulation oracles).

The above FO and REACT/GEM transformations have a couple of small but important disadvantages.

- **Tightness.** The security reduction of the FO transformation [3, 4] in the random oracle model is not tight, i.e., it loses a factor of q_G, the number of random oracle queries. A non-tight security proof results in considerably less efficient schemes. The REACT/GEM transformations have a tight security reduction. However they require the underlying encryption scheme to be OW-PCA secure. Many natural lattice-based encryption scheme are not OW-PCA secure and it is difficult to build an IND-CPA or OW-PCA secure encryption scheme from an OW-CPA secure one, with a tight security reduction.

- **Correctness error.** Both FO and REACT/GEM transformation require the underlying asymmetric encryption scheme to be perfectly correct, i.e., not having a decryption error. In general, one cannot exclude the fact that even a small decryption error could be exploited by a concrete IND-CCA attack against FO-like transformed schemes.

Note that all the figures in this report are taken from the original article [1].

2 Preliminaries

For $n \in \mathbb{N}$, let $[n] := \{1, \dots, n\}$. For a set S, $|S|$ denotes the cardinality of S. For a finite set S, we denote the sampling of a uniform random element x by $x \xleftarrow{\$} S$ and we denote the sampling according to some distribution $\mathcal{D}$ by $x \leftarrow \mathcal{D}$. By $[\![B]\!]$ we denote the bit that is 1 if the Boolean Statement B is true, and otherwise 0.
Algorithms. Denote the deterministic computation of an algorithm A on input x by $y := A(x)$. We denote algorithms with access to an oracle O by A^O. Unless stated otherwise, we assume all algorithms to be probabilistic and denote the computation by $y \leftarrow A(x)$.
Random Oracles. We will model hash functions $\mathsf{H} : \mathcal{D}_{\mathsf{H}} \to \mathcal{T}(\mathsf{H})$ as random oracles. To keep record of the queries issued to H, we will use a hash list $\mathcal{L}_{\mathsf{H}}$ that

contains all tuples $(x, \mathsf{H}(x))$ of arguments $x \in \mathcal{D}_{\mathsf{H}}$ that H was queried on and the respective answers $\mathsf{H}(x)$. We make the convention that $\mathsf{H}(x) = \perp$ for all $x \notin \mathcal{D}_{\mathsf{H}}$.

```
GAME COR:
$(pk, sk) \leftarrow \mathsf{Gen}$
$m \leftarrow \mathsf{A}(sk, pk)$
$c \leftarrow \mathsf{Enc}(pk, m)$
return $[\![\mathsf{Dec}(sk, c) = m]\!]$

GAME COR-RO:
$(pk, sk) \leftarrow \mathsf{Gen}$
$m \leftarrow \mathsf{A}^{\mathsf{G}(\cdot)}(sk, pk)$
$c \leftarrow \mathsf{Enc}(pk, m)$
return $[\![\mathsf{Dec}(sk, c) = m]\!]$
```

Figure 1: On the left there is a correctness game COR for PKE in the standard model but on the right COR-RO for PKE defined relative to a random oracle G.

In the following subsection 2.1 in the original paper the authors define and explain following parts of a public-key encryption scheme:

- Syntax - what a public-key encryption scheme $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ consist of and are the algorithms $\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}$ used;

- Correctness - what it means for a public-key encryption scheme to be δ-correct. (see figure 1). Note that the correctness definition in the standard model is a special case of the one in the random oracle model, where the number of random oracle queries is zero and hence $\delta(q_{\mathsf{G}})$ is a constant;

- Min-Entropy - For $(pk, sk) \leftarrow \mathsf{Gen}$ and $m \in \mathcal{M}$, they define the *min-entropy* of $\mathsf{Enc}(pk, m)$ by $\gamma(pk, m) := -\log \max_{c \in C} \Pr_{r \leftarrow \mathcal{R}}[c = \mathsf{Enc}(pk, m; r)]$. PKE is *$\gamma$-spread* if for every key pair $(pk, sk) \leftarrow \mathsf{Gen}$ and every message $m \in \mathcal{M}$, we have $\gamma(pk, m) \geq \gamma$.

- Security - define three security notions for public-key encryption (See Definition 1 and Figure 2).

```
GAME OW-ATK:
$(pk, sk) \leftarrow \mathsf{Gen}$
$m^* \xleftarrow{\$} \mathcal{M}$
$c^* \leftarrow \mathsf{Enc}(pk, m^*)$
$m' \leftarrow \mathsf{A}^{\mathsf{O}_{\mathsf{ATK}}}(pk, c)$
return $\textsc{Pco}(m', c^*)$

$\textsc{Pco}(m \in \mathcal{M}, c)$
return $[\![\mathsf{Dec}(sk, c) = m]\!]$

$\textsc{Cvo}(c \neq c^*)$
$m := \mathsf{Dec}(sk, c)$
return $[\![m \in \mathcal{M}]\!]$
```

Figure 2: Games OW-ATK, with ATK $\in$ {CPA, PCA, VA, PCVA} for PKE, where $Pco(\cdot, \cdot)$ is the Plaintext Checking Oracle and $Cvo(\cdot)$ is the Ciphertext Validity Oracle.

Definition 1. *(*$\mathsf{OW\text{-}ATK}$ *for* PKE*). Let* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a public-key encryption scheme with message space* $\mathcal{M}$*. For* $\mathsf{ATK} \in \{\mathsf{CPA}, \mathsf{PCA}, \mathsf{VA}, \mathsf{PCVA}\}$*, we define* $\mathsf{OW\text{-}ATK}$ *games as in Figure 2, where*

$$O_{\mathsf{ATK}} := \begin{cases} - & \mathsf{ATK} = \mathsf{CPA} \\ PCO(\cdot,\cdot) & \mathsf{ATK} = \mathsf{PCA} \\ CVO(\cdot) & \mathsf{ATK} = \mathsf{VA} \\ PCO(\cdot,\cdot), CVO(\cdot) & \mathsf{ATK} = \mathsf{PCVA} \end{cases},$$

We define the $\mathsf{OW\text{-}ATK}$ *advantage function of an adversary* A *against* PKE *as*

$$Adv^{\mathsf{OW\text{-}ATK}}_{\mathsf{PKE}}(\mathsf{A}) := Pr[\mathsf{OW\text{-}ATK}^{\mathsf{A}}_{\mathsf{PKE}} \Rightarrow 1]$$

Remarks. The definition of the plaintext checking oracle implicitly disallows queries on messages $m \in \mathcal{M}$. (that means $Pco(m \notin \mathcal{M}, c)$ yields $\perp$) This restriction is important because otherwise the ciphertext validity oracle $Cvo(\cdot)$ could be simulated as $Cvo(m) = Pco(\perp, c)$. Also, the ciphertext validity oracle implicitly disallows queries on the challenge ciphertext c^*.

Usually, the adversary wins the one-way game iff its output equals the challenge message. Instead, in game $\mathsf{OW\text{-}ATK}$ the correctness of message m' is checked using the Pco oracle, which returns 1 iff $Dec(sk, c^*) = m'$. The two games have statistical difference δ, if PKE is δ-correct.

Additionally the authors defined IND-CPA and IND-CCA. Also, OW-ATK and IND-CPA security is defined in the random oracle model, where PKE and adversary A are given access to a random oracle H.

Definition 2. *(*$\mathsf{IND\text{-}CPA}$ *for* PKE *). Let* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be a public-key encryption scheme with message space* $\mathcal{M}$*. Define the* $\mathsf{IND\text{-}CPA}$ *game as in Figure 3.*
The $\mathsf{IND\text{-}CPA}$ *advantage function of an adversary* $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ *against* PKE *(*A_2 *has binary output) as*

$$Adv^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A}) := \left| \Pr[\mathsf{IND\text{-}CPA}^{\mathsf{A}} \Rightarrow 1] - \frac{1}{2} \right|$$

```
GAME IND-CPA
$(pk, sk) \leftarrow \mathsf{Gen}$
$b \overset{\$}{\leftarrow} \{0,1\}$
$(m_0^*, m_1^*, st) \leftarrow \mathsf{A}_1(pk)$
$c^* \leftarrow \mathsf{Enc}(pk, m_b^*)$
$b' \leftarrow \mathsf{A}_2(pk, c^*, st)$
return $[\![ b' = b ]\!]$
```

```
GAME IND-CCA
$(pk, sk) \leftarrow \mathsf{Gen}$
$b \overset{\$}{\leftarrow} \{0,1\}$
$(K_0^*, c^*) \leftarrow \mathsf{Encaps}(pk)$
$K_1^* \overset{\$}{\leftarrow} \mathcal{K}$
$b' \leftarrow \mathsf{A}^{\textsc{Decaps}}(c^*, K_b^*)$
return $[\![ b' = b ]\!]$
```

```
DECAPS$(c \neq c^*)$
$K := \mathsf{Decaps}(sk, c)$
return $K$
```

Figure 3: Games IND-CPA for PKE and IND-CCA game for KEM.

Definition 3. *(*$\mathsf{IND\text{-}CCA}$ *for* KEM*). Define the* $\mathsf{IND\text{-}CCA}$ *game as in Figure 3. The* $\mathsf{IND\text{-}CCA}$ *advantage function of an adversary* A *(with a binary output) against* KEM *as*

$$Adv_{\mathsf{KEM}}^{\mathsf{IND\text{-}CCA}}(\mathsf{A}) := \left|\Pr[\mathsf{IND\text{-}CCA}^{\mathsf{A}} \Rightarrow 1] - \frac{1}{2}\right|$$

Let us explain, what these security notions really mean. Take OW-CPA, based on figure 2 we first:

1. generate public and secret keys,

2. choose a message m^* uniformly at random from the message space,

3. compute the ciphertext.

Next the adversary tries to find m based on the ciphertext c and our public key pk. If the adversary finds the correct message m, the algorithm returns 1, if not, then it returns 0. The OW-ATK advantage function is the probability, that 1 is returned. That is the probability, that the adversary finds the correct message based on the ciphertext and our public key.

With different schemes, the adversary may have access to plaintext checking oracle (OW-PCA), the ciphertext checking oracle (OW-VA) or both (OW-PCVA). In the previous example about OW-CPA, the adversary does not have access to either one of these oracles.

In IND-CPA, there are two messages m_0 and m_1, that are chosen by the adversary. The security in that case means, that given an encryption, the adversary cannot tell which one of the two messages was encrypted. IND-CCA security was defined for KEM insead of a PKE. This means that we want the encapsulation of the key to remain secret instead of some message. In the IND-CCA game on figure 3, the adversary has access to the decapsulation oracle, that is, for a $c \neq c^*$, the adversary can find the K that encaps to c. Here c^* is the encapsulation of key K_0^*. This sceme is secure if adversary cannot tell whether c^* is the encapsulation of the key K^* that he is given or not.

3 Transformations

The authors provide fine-grained transformations that can be used to turn an OW-CPA secure PKE scheme into an IND-CCA secure one in several steps. For instance, they provide separate OW-CPA → OW-PCA and OW-PCA → IND-CCA transformations that, taken together, yield the original FO transformation.

The authors also provide multiple variants of these transformations that achieve different security goals and tightness properties that are robust against PKE schemes with correctness errors (in the sense that the correctness error of the original scheme bounds the correctness error of the resulting schemes).

Before talking about the transformations in detail, the authors remark that all transformations require a PKE scheme (and not a KEM) and they view it as an interesting open problem to construct similar transformations that only assume KEMs, because of the potential of additional efficiency gain.

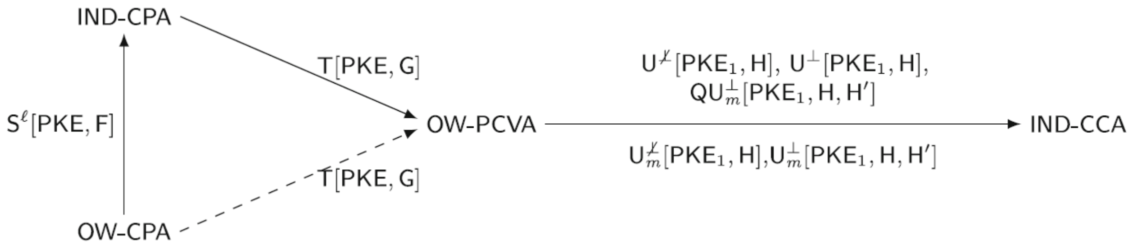
IND-CPA
T[PKE, G]
S^{ℓ}[PKE, F]
OW-PCVA
T[PKE, G]
OW-CPA
$\mathsf{U}^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}]$, $\mathsf{U}^{\perp}[\mathsf{PKE}_1, \mathsf{H}]$,
$\mathsf{QU}^{\perp}_{m}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$
$\mathsf{U}^{\not\perp}_{m}[\mathsf{PKE}_1, \mathsf{H}]$,$\mathsf{U}^{\perp}_{m}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$
IND-CCA

Figure 4: The modular transformations. Solid arrows indicate tight reductions, dashed arrows indicate non-tight reductions.

Transformation	**Security implication**	**QROM?**	**ROM Tightness?**	**Requirements**
$\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ (§3.1)	OW-CPA ⇒ OW-PCA	✓	—	none
$\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ (§3.1)	IND-CPA ⇒ OW-PCA	✓	✓	none
$\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ (§3.1)	OW-CPA ⇒ OW-PCVA	✓	—	γ-spread
$\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ (§3.1)	IND-CPA ⇒ OW-PCVA	—	✓	γ-spread
$\mathsf{KEM}^{\not\perp} = \mathsf{U}^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}]$ (§3.2)	OW-PCA ⇒ IND-CCA	—	✓	none
$\mathsf{KEM}^{\perp} = \mathsf{U}^{\perp}[\mathsf{PKE}_1, \mathsf{H}]$ (§3.2)	OW-PCVA ⇒ IND-CCA	—	✓	none
$\mathsf{KEM}^{\not\perp}_{m} = \mathsf{U}^{\not\perp}_{m}[\mathsf{PKE}_1, \mathsf{H}]$ (§3.2)	OW-CPA ⇒ IND-CCA	—	✓	det. PKE_1
$\mathsf{KEM}^{\perp}_{m} = \mathsf{U}^{\perp}_{m}[\mathsf{PKE}_1, \mathsf{H}]$ (§3.2)	OW-VA ⇒ IND-CCA	—	✓	det. PKE_1
$\mathsf{QKEM}^{\perp}_{m} = \mathsf{QU}^{\perp}_{m}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$ (§4.3)	OW-PCA ⇒ IND-CCA	✓	✓	none
$\mathsf{PKE}_{\ell} = \mathsf{S}^{\ell}[\mathsf{PKE}, \mathsf{F}]$ (§3.4)	OW-CPA ⇒ IND-PCA	—	✓	none

Figure 5: Properties of the transformations. The tightness row only refers to tightness in the standard random oracle model; reductions in the quantum random oracle model are non-tight.

All the security reductions of the transformations can be found in Figure 5. Now we give you more detailed descriptions of the transformations.

T: from OW-CPA to OW-PCA security (*"Derandomization"* + *"Re-encryption"*). T is Encrypt-with-Hash construction: From an encryption scheme PKE and a hash function G, we build a deterministic encryption scheme $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$ by

$$\mathsf{Enc}_1(pk, m) := \mathsf{Enc}(pk, m; \mathsf{G}(m)),$$

where $\mathsf{G}(m)$ is used as random coins for Enc. If ROM is tight, we get OW-PCA security from a IND-CPA secure PKE. If PKE is γ-spread, then PKE_1 is even OW-PCVA secure. Let us note that OW-PCVA security in Figure 5 is PCA security where the adversary additionally has access to a validity oracle $Cvo(c)$. Validity oracle is used to check that c does not decrypt to $\perp$ (the validity of c).

$\mathsf{U}^{\not\perp}$ ($\mathsf{U}^{\perp}$): from OW-PCA (OW-PCVA) to IND-CCA security (*"Hashing"*). From an encryption scheme PKE_1 and a hash function H, we build a key encapsulation mechanism $\mathsf{KEM}^{\not\perp} = \mathsf{U}^{\not\perp}[\mathsf{PKE}_1, \mathsf{H}]$ with "implicit rejection" by

$$\mathsf{Encaps}(pk) := (c \leftarrow \mathsf{Enc}_1(pk, m), K := \mathsf{H}(c, m)),$$

where m is picked at random from the message space.

$$\mathsf{Decaps}^{\not\perp}(sk, c) = \begin{cases} \mathsf{H}(c, m) & m \neq \perp \\ \mathsf{H}(c, s) & m = \perp \end{cases},$$

where $m := \mathsf{Dec}(sk, c)$ and s is a random seed which is contained in sk.

Authors also defined $\mathsf{KEM}^{\perp} = \mathsf{U}^{\perp}[\mathsf{PKE}_1, \mathsf{H}]$ with "explicit rejection". It differs from $\mathsf{KEM}^{\not\perp}$ only in decapsulation:

$$\mathsf{Decaps}^{\perp}(sk, c) = \begin{cases} \mathsf{H}(c, m) & m \neq \perp \\ \perp & m = \perp \end{cases},$$

where $m := \mathsf{Dec}(sk, c)$.

So $\mathsf{U}^{\not\perp}$ gives us security from OW-PCA to IND-CCA and $\mathsf{U}^{\perp}$ from OW-PCVA to IND-CCA.

$\mathsf{U}^{\not\perp}_m$ ($\mathsf{U}^{\perp}_m$): from deterministic OW-PCA (OW-VA) to IND-CCA security (*"Hashing"*). Transformation $\mathsf{U}^{\not\perp}_m$ ($\mathsf{U}^{\perp}_m$) is a variant of $\mathsf{U}^{\not\perp}$ ($\mathsf{U}^{\perp}$), where $K = \mathsf{H}(c, m)$ is replaced by $K = \mathsf{H}(m)$. OW-VA security is OW-CPA security, where the adversary is given access to a validity oracle.

The authors define multiple variants of transformation U, because it gives a larger variety of possible combined transformations that have different requirements and properties. They remark that all previous variants of the FO transformation require the underlying PKE scheme to be γ-spread, which means that ciphertexts have sufficiently large entropy. Not all transformations described in this paper need this property. For example, combining two results about the transformations T and $\mathsf{U}^{\not\perp}$, we can show that the original FO transformation yields IND-CCA security from IND-CPA security with a tight security reduction. On the other hand combining T and $\mathsf{U}^{\perp}$, yields IND-CCA security from the weaker OW-CPA security but without a tight security reduction. But at the same time the encryption scheme PKE needs to be γ-spread.

The modular treatment also makes it easier to prove the security of the transformations (instead of having one big proof we have many smaller ones). On the other hand, having so many different notations may confuse some readers.

$\mathsf{QU}_m^{\perp}$: from OW-PCA to IND-CCA security in the QROM. First the authors prove that transformation T also works in the quantum random oracle model. Next, they build a key encapsulation mechanism $\mathsf{QKEM}_m^{\perp} = \mathsf{QU}_m^{\perp}[\mathsf{PKE}_1, \mathsf{H}, \mathsf{H}']$ with explicit rejection by defining

$$\mathsf{QEncaps}_m(pk) := (\underbrace{(c \leftarrow \mathsf{Enc}_1(pk, m), d := \mathsf{H}'(m))}_{\text{ciphertext}}, \underbrace{K := \mathsf{H}(m)}_{\text{encapsulated key}}),$$

where m is picked at random from the message space and

$$\mathsf{QDecaps}_m^{\perp}(sk, c, d) = \begin{cases} \mathsf{H}(m') & m' \neq \perp \\ \perp & m' = \perp \vee \mathsf{H}'(m') \neq d \end{cases},$$

where $m' := \mathsf{Dec}(sk, c)$. So, $\mathsf{QU}_m^{\perp}$ differs from $\mathsf{U}^{\perp}$ only in the additional hash value d from the ciphertext. Here, H' is a random oracle with matching domain and image.

These transformations are used for the final FO transformations in the following way:

Transformation	**QROM?**	**ROM Tightness?**	**Requirements**
$\mathsf{FO}^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}] := \mathsf{U}^{\not\perp}[\mathsf{T}[\mathsf{PKE}, \mathsf{G}], \mathsf{H}]$	—	✓	none
$\mathsf{FO}^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}] := \mathsf{U}^{\perp}[\mathsf{T}[\mathsf{PKE}, \mathsf{G}], \mathsf{H}]$	—	✓	γ-spread
$\mathsf{FO}_m^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}] := \mathsf{U}_m^{\not\perp}[\mathsf{T}[\mathsf{PKE}, \mathsf{G}], \mathsf{H}]$	—	✓	none
$\mathsf{FO}_m^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}] := \mathsf{U}_m^{\perp}[\mathsf{T}[\mathsf{PKE}, \mathsf{G}], \mathsf{H}]$	—	✓	γ-spread
$\mathsf{QFO}_m^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}, \mathsf{H}'] := \mathsf{QU}_m^{\perp}[\mathsf{T}[\mathsf{PKE}, \mathsf{G}], \mathsf{H}, \mathsf{H}']$	✓	✓	none

As a result they obtain that IND-CCA security of $\mathsf{FO}^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$, $\mathsf{FO}^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$, $\mathsf{FO}_m^{\not\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$ and $\mathsf{FO}_m^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}]$ non-tightly reduces to the OW-CPA security of PKE, and tightly reduces to the IND-CPA security of PKE, in the random oracle model. Further, IND-CCA security of $\mathsf{QFO}_m^{\perp}[\mathsf{PKE}, \mathsf{G}, \mathsf{H}, \mathsf{H}']$ reduces to the OW-CPA security of PKE, in the quantum random oracle model. As it is common in the quantum random oracle model, all of the reductions are (highly) non-tight and authors leave it as an open problem to derive a tighter security reduction of T.

Transformation S^l : From OW-CPA to IND-CPA, Tightly. Transformation S^l offers the following tradeoff between efficiency and tightness, in case one needs to rely on OW-CPA security instead of IND-CPA security. S^l transforms an OW-CPA secure PKE into an IND-CPA secure PKE_l, where l is a parameter.

$$\mathsf{Enc}_l(pk, m) := (\mathsf{Enc}(pk, x_1), \dots, \mathsf{Enc}(pk, x_l), m \oplus \mathsf{G}(x_1, \dots, x_l)).$$

The reduction loses a factor of $q_{\mathsf{G}}^{1/l}$, where q_{G} is the number of G-queries an adversary makes.

4 Modular FO Transformations

Next we introduce one of the transformations mentioned in the previous section: transformation T, that transforms any OW-CPA secure encryption scheme PKE into a OW-PCA secure encryption scheme PKE_1.

Transformation T: From OW-CPA/IND-CPA to OW-PCVA.
As mentioned in the previous sections, transformation T satisfies different security notations based on the properties of the underlying encryption scheme PKE. Let us look at the case where PKE is OW-CPA secure. Also assume, that PKE γ-spread. In this case T transforms the public-key encryption scheme into an OW-PCVA secure one.

```
Enc_1(pk, m)
  $c := \mathsf{Enc}(pk, m; \mathsf{G}(m))$
  return $c$

Dec_1(sk, c)
  $m' := \mathsf{Dec}(sk, c)$.
  if $m' = \perp$ or $\mathsf{Enc}(pk, m'; \mathsf{G}(m')) \neq c$
      return $\perp$
  else return $m'$
```

Figure 6: OW-PCVA-secure encryption scheme $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$.

The construction. Take $\mathsf{PKE}_1 = \mathsf{T}[\mathsf{PKE}, \mathsf{G}]$, where public-key encryption scheme $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ has message space $\mathcal{M}$ and randomness space $\mathcal{R}$, and a random oracle $\mathsf{G} : \mathcal{M} \to \mathcal{R}$. The algorithms of $\mathsf{PKE}_1 = (\mathsf{Gen}, \mathsf{Enc}_1, \mathsf{Dec}_1)$ are defined in Figure 6. Note that the resulting encryption is deterministic (it always produces the same ciphertext for a given message and public key). The decryption returns a message only if the encryption of the decrypted message gives back the correct ciphertext c. Otherwise $\perp$ is returned.

Let us try to give some intuition about why using randomness that depends on the message (that is $\mathsf{G}(m)$) is useful. The meaning of OW-PCA is that a ciphertext can be created only if you know the plaintext. But the weaker notion of OW-CPA does not guarantee that. Take ElGamal encryption scheme, for example. During the encryption we find $Enc(pk, m) = (g^r, m \cdot h^r)$. Since r is randomly chosen, any two random group elements form a valid ciphertext. But, after applying transformation T, the encryption would give $Enc(pk, m) = (g^{\mathsf{G}(m)}, m \cdot h^{\mathsf{G}(m)})$. Since both parts of the ciphertext now depend on the message m, two random group elements will not work anymore (with high probability).

The following theorem from [1] establishes the security of PKE_1 that we just described.

Theorem 1. *(PKE $\mathsf{OW\text{-}CPA}$ $\xrightarrow{ROM}$ PKE_1 $\mathsf{OW\text{-}PCVA}$) If PKE is δ-correct, then*

PKE_1 *is* δ_1*-correct in the random oracle model with* $\delta_1(q_\mathsf{G}) = q_\mathsf{G} \cdot \delta$. *Assume* PKE *to be* γ*-spread. Then, for any* OW-PCVA *adversary* B *that issues at most* q_G *queries to the random oracle* G*,* q_P *queries to a plaintext checking oracle* Pco*, and* q_V *queries to a validity checking oracle* Cvo*, there exists an* OW-CPA *adversary* A *such that*

$$Adv^{\mathsf{OW\text{-}PCVA}}_{\mathsf{PKE}_1}(\mathsf{B}) \leq q_\mathsf{G} \cdot \delta + q_\mathsf{V} \cdot 2^{-\gamma} + (q_\mathsf{G} + 1) \cdot Adv^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$$

and the running time of A *is about that of* B.

This theorem consists of two parts. Let us prove the first part, which says that if PKE is δ-correct, then PKE_1 is δ_1-correct in the random oracle model with $\delta_1(q_\mathsf{G}) = q_\mathsf{G} \cdot \delta$.

Proof. Consider an adversary A playing the correctness game COR-RO (figure 1) of PKE_1 in the random oracle model. We know that adversary issues at most q_G (distinct) queries $\mathsf{G}(m_1), \ldots, \mathsf{G}(m_{q_\mathsf{G}})$ to G. Call such a query $\mathsf{G}(m_i)$ *problematic* iff it exhibits a correctness error in PKE_1 (that means $Dec(sk, Enc(pk, m_i; \mathsf{G}(m_i))) \neq m_i$). Since the random oracle G outputs independently random variables, each $\mathsf{G}(m_i)$ is problematic with probability at most δ. That is because PKE is δ-correct. Now, if we want the probability that at least one $\mathsf{G}(m_i)$ is problematic, we take union of the bounds, that is $q_\mathsf{G} \cdot \delta$. This proves that PKE_1 is δ_1-correct in the random oracle model with $\delta_1(q_\mathsf{G}) = q_\mathsf{G} \cdot \delta$.

For the full proof see [2], but the main idea of the second part of the proof is that since Enc_1 is deterministic, the $\mathsf{PCA}(\cdot,\cdot)$ oracle can be equivalently implemented by "re-encryption". This means that $Dec(sk, c)$ first decrypts c into m' and rejects if $Enc(pk, m', \mathsf{G}(m') \neq c)$. The $Cvo(\cdot)$ oracle can be implemented by controlling the random oracles. $Cvo(c)$ usually finds the decyption m' of a ciphertext c, checks that m' is in the message space and that encryption the message m' gives back the correct c. Instead this can be equivalently implemented by finding $(m, \mathsf{G}(m))$ from hash list and checking that $Enc(pk, m; \mathsf{G}(m) = c)$. The hash list contains all tuples $(x, \mathsf{G}(x))$ that G was queried on.

By definition, OW-PCA security is OW-PCVA security with no queries to the validity checking oracle ($q_\mathsf{V} := 0$). Hence, the bound of Theorem 1 shows that PKE_1 is OW-PCA secure, without requiring PKE to be γ-spread. So this theorem gives us two transformations from figure 5. For detailed descriptions and proofs about the other transformations $\mathsf{U}^{\not\perp}$,$\mathsf{U}^{\not\perp}_m$, $\mathsf{U}^{\perp}$,$\mathsf{U}^{\perp}_m$, see [2].

4.1 The Resulting KEMs

For completeness, the authors combine transformation T with $\{\mathsf{U}^{\not\perp}$,$\mathsf{U}^{\not\perp}_m$, $\mathsf{U}^{\perp}$,$\mathsf{U}^{\perp}_m\}$ to obtain four variants of the FO transformations:

$$\begin{aligned}
\mathsf{KEM}^{\not\perp} &= \mathsf{FO}^{\not\perp}[\mathsf{PKE},\mathsf{G},\mathsf{H}] := \mathsf{U}^{\not\perp}[\mathsf{T}[\mathsf{PKE},\mathsf{G}],\mathsf{H}] = (\mathsf{Gen}^{\not\perp},\mathsf{Encaps},\mathsf{Decaps}^{\not\perp})\\
\mathsf{KEM}^{\perp} &= \mathsf{FO}^{\perp}[\mathsf{PKE},\mathsf{G},\mathsf{H}] := \mathsf{U}^{\perp}[\mathsf{T}[\mathsf{PKE},\mathsf{G}],\mathsf{H}] = (\mathsf{Gen},\mathsf{Encaps},\mathsf{Decaps}^{\perp})\\
\mathsf{KEM}^{\not\perp}_m &= \mathsf{FO}^{\not\perp}_m[\mathsf{PKE},\mathsf{G},\mathsf{H}] := \mathsf{U}^{\not\perp}_m[\mathsf{T}[\mathsf{PKE},\mathsf{G}],\mathsf{H}] = (\mathsf{Gen}^{\not\perp},\mathsf{Encaps}_m,\mathsf{Decaps}^{\not\perp}_m)\\
\mathsf{KEM}^{\perp}_m &= \mathsf{FO}^{\perp}_m[\mathsf{PKE},\mathsf{G},\mathsf{H}] := \mathsf{U}^{\perp}_m[\mathsf{T}[\mathsf{PKE},\mathsf{G}],\mathsf{H}] = (\mathsf{Gen},\mathsf{Encaps}_m,\mathsf{Decaps}^{\perp}_m)\ .
\end{aligned}$$

The following table provides (simplified) concrete bounds of the IND-CCA security of KEM. The left column provides the bounds relative to the OW-CPA advantage and the right column relative to IND-CPA advantage.

KEM	Concrete bounds on $\mathrm{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathsf{KEM}}(\mathsf{B}) \leq$	
$\mathsf{KEM}^{\not\perp}$	$q_{\mathsf{RO}} \cdot \delta + \frac{2q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 2q_{\mathsf{RO}} \cdot \mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$	$q_{\mathsf{RO}} \cdot \delta + \frac{3q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 3 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A}')$
$\mathsf{KEM}^{\perp}$	$q_{\mathsf{RO}} \cdot (\delta + 2^{-\gamma}) + 2q_{\mathsf{RO}} \cdot \mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$	$q_{\mathsf{RO}} \cdot \left(\delta + 2^{-\gamma}\right) + \frac{3q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 3 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A}')$
$\mathsf{KEM}^{\not\perp}_m$	$(2q_{\mathsf{RO}} + q_D) \cdot \delta + \frac{2q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 2q_{\mathsf{RO}} \cdot \mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$	$(2q_{\mathsf{RO}} + q_D) \cdot \delta + \frac{3q_{\mathsf{RO}}}{\lvert\mathcal{M}\rvert} + 3 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A}')$
$\mathsf{KEM}^{\perp}_m$	$(2q_{\mathsf{RO}} + q_D) \cdot \delta + q_{\mathsf{RO}} \cdot 2^{-\gamma} + 2q_{\mathsf{RO}} \cdot \mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})$	$(2q_{\mathsf{RO}} + q_D) \cdot \delta + q_{\mathsf{RO}} \cdot 2^{-\gamma} + 3 \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A}')$

5 Modular FO Transformation in the QROM

In this section, we will revisit the transformations in the quantum random oracle model (QROM). The following transformations hold:

- Transformation T: From OW-CPA to OW-PCA in the QROM
- Transformation $\mathsf{QU}^{\perp}_m$: From OW-PCA to IND-CCA in the QROM.
- Transformation $\mathsf{QU}^{\not\perp}_m$: From OW-PCA to IND-CCA in the QROM.

Combining these transformations gives following KEMs:

$$\begin{aligned}
\mathsf{QKEM}^{\perp}_m &= \mathsf{QFO}^{\perp}_m[\mathsf{PKE},\mathsf{G},\mathsf{H},\mathsf{H}'] := \mathsf{QU}^{\perp}_m[\mathsf{T}[\mathsf{PKE},\mathsf{G}],\mathsf{H},\mathsf{H}']\\
&= (\mathsf{Gen},\mathsf{QEncaps}_m,\mathsf{QDecaps}^{\perp}_m)\\
\mathsf{QKEM}^{\not\perp}_m &= \mathsf{QFO}^{\not\perp}_m[\mathsf{PKE},\mathsf{G},\mathsf{H},\mathsf{H}'] := \mathsf{QU}^{\not\perp}_m[\mathsf{T}[\mathsf{PKE},\mathsf{G}],\mathsf{H},\mathsf{H}']\\
&= (\mathsf{Gen}^{\not\perp},\mathsf{QEncaps}_m,\mathsf{QDecaps}^{\not\perp}_m).
\end{aligned}$$

As a final result, the authors provide (simplified) concrete bounds of IND-CCA security of $\mathsf{KEM} \in \{\mathsf{QKEM}^{\not\perp}_m, \mathsf{QKEM}^{\perp}_m\}$ in the quantum random oracle model, in the following table.

KEM	Concrete bound on $\mathrm{Adv}^{\mathsf{IND\text{-}CCA}}_{\mathsf{KEM}}(\mathsf{B}) \leq$
$\mathsf{QKEM}^{\not\perp}_m$, $\mathsf{QKEM}^{\perp}_m$	$8q_{\mathsf{RO}}\sqrt{\delta \cdot q_{\mathsf{RO}}^2 + q_{\mathsf{RO}} \cdot \sqrt{\mathrm{Adv}^{\mathsf{OW\text{-}CPA}}_{\mathsf{PKE}}(\mathsf{A})}}$

References

[1] Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the Fujisaki-Okamoto transformation. Springer (2017). https://link.springer.com/chapter/10.1007/978-3-319-70500-2_12

[2] Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the Fujisaki-Okamoto transformation. Cryptology ePrint Archive, Report 2017/604 (2017). https://eprint.iacr.org/2017/604

[3] Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-134

[4] Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. J. Cryptol. 26(1), 80–101 (2013)

[5] Okamoto, T., Pointcheval, D.: REACT: rapid enhanced-security asymmetric cryptosystem transform. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 159–174. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45353-913

[6] Coron, J.S., Handschuh, H., Joye, M., Paillier, P., Pointcheval, D., Tymen, C.: GEM: a generic chosen-ciphertext secure encryption method. In: Preneel, B. (ed.) CT-RSA 2002. LNCS, vol. 2271, pp. 263–276. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45760-718